

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-313667

(43)Date of publication of application : 09.11.2001

(51)Int.Cl. H04L 12/54
H04L 12/58
G09C 1/00
H04L 12/22

(21)Application number : 2000-130677

(71)Applicant : RICOH CO LTD
NEW MEDIA DEVELOPMENT ASSOCIATION

(22)Date of filing : 28.04.2000

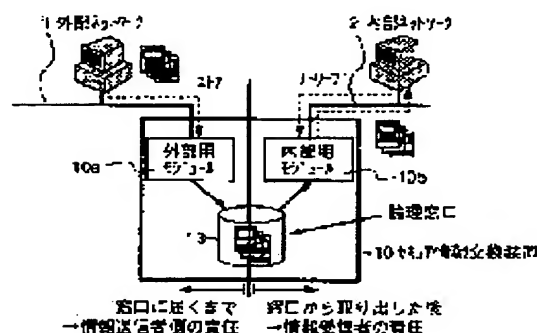
(72)Inventor : KANAI YOICHI
YANAIDA MASUYOSHI

(54) SYSTEM AND METHOD FOR EXCHANGING SECURE INFORMATION AND COMPUTER READABLE RECORDING MEDIUM FOR RECORDING PROGRAM TO MAKE COMPUTER PERFORM THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To efficiently exchange information between networks while relieving the burden of manual labor and keeping independency in the networks.

SOLUTION: A system is provided with a secure information exchange device 10 for storing exchange data in a large capacity storage device 13 when an external module 10a receives exchange data from an external network 1, taking out exchange data corresponding to a takeout request from the device 13 when an internal module 10b receives the exchange data takeout request from an internal network 2 and outputting it.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2001-313667

(P 2001-313667 A)

(43) 公開日 平成13年11月9日 (2001. 11. 9)

(51) Int. Cl. 7	識別記号	F I	テーマコード (参考)
H 0 4 L 12/54		G 0 9 C 1/00	6 4 0 A 5J104
	12/58		6 6 0 E 5K030
G 0 9 C 1/00	6 4 0	H 0 4 L 11/20	1 0 1 B 9A001
	6 6 0		11/26
H 0 4 L 12/22			
審査請求 未請求 請求項の数 2 4		O L	(全 2 9 頁)

(21) 出願番号 特願2000-130677 (P2000-130677)

(22) 出願日 平成12年4月28日 (2000. 4. 28)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(71) 出願人 596062738

財団法人ニューメディア開発協会

東京都港区三田1-4-28

(72) 発明者 金井 洋一

東京都大田区中馬込1丁目3番6号 株式会
社リコー内

(74) 代理人 100104190

弁理士 酒井 昭徳

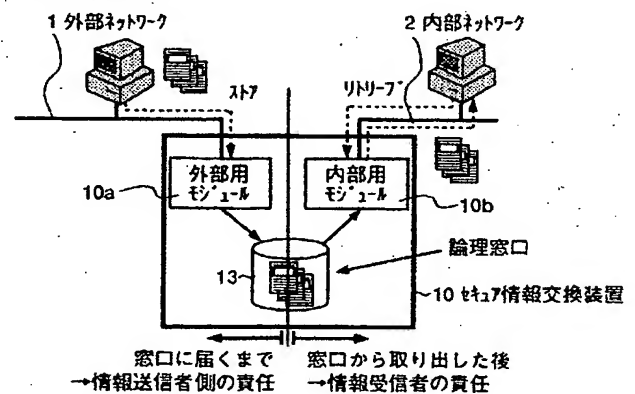
最終頁に続く

(54) 【発明の名称】 セキュア情報交換システム、セキュア情報交換方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうこと

【解決手段】 外部用モジュール10aが外部ネットワーク1から交換データを受け付けた際に、該交換データを大容量記憶装置13に格納し、内部用モジュール10bが内部ネットワーク2から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを大容量記憶装置13から取り出して出力するセキュア情報交換装置10を設ける。



【特許請求の範囲】

【請求項1】 第1のネットワーク上に位置する第1の端末装置と第2のネットワーク上に位置する第2の端末装置との間で情報交換をおこなうセキュア情報交換システムにおいて、

前記第1の端末装置または第2の端末装置から受け付けた交換データを一時記憶する記憶手段と、

前記第1の端末装置から交換データを受け付けた際に、該交換データを前記記憶手段に格納する第1のモジュールと、

前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶手段から取り出して当該第2の端末装置に出力する第2のモジュールと、

からなるセキュア情報交換装置を前記第1のネットワークおよび第2のネットワークの間に配設したことを特徴とするセキュア情報交換システム。

【請求項2】 前記第1のモジュールは、前記第1の端末装置から交換データを受け付ける受付手段と、

前記受付手段により受け付けられた交換データについての第1の改ざん検知コードを算定する第1の算定手段と、

前記第1の算定手段により算定された第1の改ざん検知コードを当該交換データと対応づけて前記記憶手段に格納する第1の格納手段と、

を備え、

前記第2のモジュールは、

前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを前記記憶手段から取り出す取出手段と、

前記取出手段により取り出された第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第1の検証手段と、

を備えたことを特徴とする請求項1に記載のセキュア情報交換システム。

【請求項3】 前記第1のモジュールは、複数の交換データを含むリストについての第2の改ざん検知コードを算定する第2の算定手段と、前記第2の算定手段により算定された第2の改ざん検知コードを前記リストとともに前記記憶手段に格納する第2の格納手段と、

を備え、前記第2のモジュールは、前記第2の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第2の検証手段をさらに備えたことを特徴とする請求項2に記載のセキュア情報交換システム。

【請求項4】 前記第1のモジュールおよび第2のモジュールは、前記記憶手段に記憶した交換データの編集要求並びに削除要求を拒否する拒否手段をさらに備えたこ

とを特徴とする請求項1、2または3に記載のセキュア情報交換システム。

【請求項5】 前記第1のモジュールは、

前記第1の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成する作成手段と、

前記受取証作成手段により作成された受取証データを前記第1の端末装置に返送する返送手段と、

をさらに備えたことを特徴とする請求項1～4のいずれか一つに記載のセキュア情報交換システム。

【請求項6】 前記作成手段は、前記交換データの特徴量を含む受取証データを作成することを特徴とする請求項5に記載のセキュア情報交換システム。

【請求項7】 前記作成手段は、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする請求項5または6に記載のセキュア情報交換システム。

【請求項8】 前記作成手段は、前記受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成することを特徴とする請求項5、6または7に記載のセキュア情報交換システム。

【請求項9】 前記第1のモジュールは、

前記第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第2の端末装置に送出済みであるか否かを確認する送出確認手段と、

前記送出確認手段による確認結果を前記第1の端末装置に通知する送出確認通知手段と、

をさらに備えたことを特徴とする請求項5～8のいずれか一つに記載のセキュア情報交換システム。

【請求項10】 前記第1のモジュールは、

前記第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶手段に記憶されているか否かを確認する記憶確認手段と、

前記記憶確認手段により前記記憶手段に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶手段から削除する削除手段と、

前記交換データの削除の有無を前記第1の端末装置に通知する削除通知手段と、

をさらに備えたことを特徴とする請求項5～9のいずれか一つに記載のセキュア情報交換システム。

【請求項11】 前記第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードは、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする請求項1～10のいずれか一つに記載のセキュア情報交換システム。

【請求項12】 前記第1のモジュールおよび第2のモジュールは、耐タンパー性を有する筐体に格納されたこ

とを特徴とする請求項1～11のいずれか一つに記載のセキュア情報交換システム。

【請求項13】 第1のネットワーク上に位置する第1の端末装置と第2のネットワーク上に位置する第2の端末装置との間で情報交換をおこなうセキュア情報交換方法において、

前記第1の端末装置から交換データを受け付けた際に、該交換データを所定の記憶部に格納する格納工程と、前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶部から取り出して当該第2の端末装置に出力する出力工程と、

を含んだことを特徴とするセキュア情報交換方法。

【請求項14】 前記格納工程は、

前記第1の端末装置から交換データを受け付ける受付工程と、

前記受付工程により受け付けられた交換データについての第1の改ざん検知コードを算定する第1の算定工程と、

前記第1の算定工程により算定された第1の改ざん検知コードを当該交換データと対応づけて前記記憶部に格納する第1の格納工程と、

を含み、

前記出力工程は、

前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを前記記憶部から取り出す取出工程と、

前記取出工程により取り出された第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第1の検証工程と、

を含んだことを特徴とする請求項13に記載のセキュア情報交換方法。

【請求項15】 前記格納工程は、

複数の交換データを含むリストについての第2の改ざん検知コードを算定する第2の算定工程と、

前記第2の算定工程により算定された第2の改ざん検知コードを前記リストとともに前記記憶部に格納する第2の格納工程と、

を含み、

前記出力工程は、前記第2の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第2の検証工程をさらに含んだことを特徴とする請求項14に記載のセキュア情報交換方法。

【請求項16】 前記記憶部に記憶した交換データの編集要求並びに削除要求を拒否する拒否工程をさらに含んだことを特徴とする請求項13、14または15に記載のセキュア情報交換方法。

【請求項17】 前記格納工程は、

前記第1の端末装置から交換データを受け付けた際に、

該交換データの受け取りを証明する受取証データを作成する作成工程と、

前記受取証作成工程により作成された受取証データを前記第1の端末装置に返送する返送工程と、

をさらに含んだことを特徴とする請求項13～16のいずれか一つに記載のセキュア情報交換方法。

【請求項18】 前記作成工程は、前記交換データの特徴量を含む受取証データを作成することを特徴とする請求項17に記載のセキュア情報交換方法。

10 【請求項19】 前記作成工程は、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする請求項17または18に記載のセキュア情報交換方法。

【請求項20】 前記作成工程は、前記受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成することを特徴とする請求項17、18または19に記載のセキュア情報交換方法。

【請求項21】 前記格納工程は、

20 前記第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第2の端末装置に送出済みであるか否かを確認する送出確認工程と、

前記送出確認工程による確認結果を前記第1の端末装置に通知する送出確認通知工程と、

をさらに含んだことを特徴とする請求項17～20のいずれか一つに記載のセキュア情報交換方法。

【請求項22】 前記格納工程は、

30 前記第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶部に記憶されているか否かを確認する記憶確認工程と、

前記記憶確認工程により前記記憶部に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶部から削除する削除工程と、

前記交換データの削除の有無を前記第1の端末装置に通知する削除通知工程と、

をさらに含んだことを特徴とする請求項17～21のいずれか一つに記載のセキュア情報交換方法。

40 【請求項23】 前記第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードは、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする請求項13～22のいずれか一つに記載のセキュア情報交換方法。

【請求項24】 前記請求項13～23に記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

50 【発明の属する技術分野】この発明は、第1のネットワ

ーク上に位置する第1の端末装置と第2のネットワーク上に位置する第2の端末装置との間で情報交換をおこなうセキュア情報交換システム、セキュア情報交換方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができるセキュア情報交換システム、セキュア情報交換方法、および方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】現在のネットワークシステムでは、ルータやゲートウェイなどを介してネットワークを互いに接続してネットワーク間の情報伝達がなされることが多い。このため、広域にわたって情報伝達が可能となる反面、プライバシー保護、情報漏洩および不正アクセスなどが問題となる。

【0003】したがって、ネットワーク上に企業や公的機関の根幹をなす重要なデータが存在する場合には、このネットワークをインターネットなどの他のネットワークシステムと接続することが好ましくない。たとえば、人事データベースなどがある企業の基幹系ネットワークは、一般の事務系ネットワークと接続するのは好ましくないし、地方自治体における住民データが存在する基幹系ネットワークについても事務系ネットワークと接続するのは好ましくない。

【0004】しかしながら、事務系ネットワーク上でおこなった業務処理結果を基幹系ネットワークに反映したり、事務系ネットワーク側の業務処理の中で基幹系ネットワーク上のデータを使用することができれば、業務効率が改善するのもまた事実である。

【0005】このため、従来は、かかる場合に一方のネットワークでフロッピー（登録商標）ディスクなどのオフラインメディアにデータを保存し、他方のネットワークでそのデータを読み出すことにより、双方のネットワークの独立性を担保しつつ情報交換を可能にしている。

【0006】ところが、かかる人手を介した情報交換をおこなっていたのでは、データ取得に時間を要し、また情報交換にかかる人的負担も大きい。最近では、ファイアウォールを介してネットワークを接続し、許可されたプロトコルのみを中継または通過させるようにしてセキュリティを保持したまま情報交換をおこなうことが多い。

【0007】このファイアウォールは、パケットの通過／遮断をおこなうパケットフィルタリングサービスと、社内クライアントのインターネットアクセスなどを代行するプロキシ（Proxy）サービスとに大別され、OSI（Open Systems Interconnection）参照モデルのネットワーク層やアプリケ

ーション層などで機能するものが知られている。

【0008】

【発明が解決しようとする課題】しかしながら、かかるファイアウォールによれば、不正なプロトコルを用いて一方のネットワークから他方のネットワークへ入ることはできないが、正しいプロトコルさえ用いれば他方のネットワークに進入可能な仕組み（ストア・フォワード型）となるので、双方のネットワークの独立性を保つことができなくなるという問題があった。

【0009】図23は、従来の典型的なファイアウォールの概念を説明するための説明図であり、同図に示す内部ネットワークは、外部ネットワークから直接的に作用される受動的なものとなるので、ネットワークの独立性を保つことができなくなるのである。

【0010】また、外部ネットワークから内部ネットワークに情報交換用のデータを送信した場合に、どの時点でデータが受け渡しされたとするかが明確でないで、情報交換の途中でデータが改ざんまたは紛失すると、送信者側が悪いのか受信者側が悪いのか、どちらのネットワークに責任があるのかが不明確になるという問題もあった。

【0011】これらのことから、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換をいかに効率よくおこなうかが極めて重要な課題となっている。

【0012】この発明は、上述した従来技術による問題点を解決するためになされたものであり、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができるセキュア情報交換システム、セキュア情報交換方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項1に記載の発明にかかるセキュア情報交換システムは、第1のネットワーク上に位置する第1の端末装置と第2のネットワーク上に位置する第2の端末装置との間で情報交換をおこなうセキュア情報交換システムにおいて、前記第1の端末装置または第2の端末装置から受け付けた交換データを一時記憶する記憶手段と、前記第1の端末装置から交換データを受け付けた際に、該交換データを前記記憶手段に格納する第1のモジュールと、前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶手段から取り出して当該第2の端末装置に出力する第2のモジュールと、かかるセキュア情報交換装置を前記第1のネットワークおよび第2のネットワークの間に配設したことを特徴とする。

【0014】この請求項1に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データを記憶手段に格納し、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶手段から取り出して当該第2の端末装置に出力するセキュア情報交換装置を第1のネットワークおよび第2のネットワークの間に配設することとしたので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができる。

【0015】また、請求項2に記載の発明にかかるセキュア情報交換システムは、請求項1に記載の発明において、前記第1のモジュールが、前記第1の端末装置から交換データを受け付ける受付手段と、前記受付手段により受け付けられた交換データについての第1の改ざん検知コードを算定する第1の算定手段と、前記第1の算定手段により算定された第1の改ざん検知コードを当該交換データと対応づけて前記記憶手段に格納する第1の格納手段と、を備え、前記第2のモジュールが、前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを前記記憶手段から取り出す取出手段と、前記取出手段により取り出された第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第1の検証手段と、を備えたことを特徴とする。

【0016】この請求項2に記載の発明によれば、第1のモジュールでは、第1の端末装置から交換データを受け付け、受け付けた交換データについての第1の改ざん検知コードを算定し、算定した第1の改ざん検知コードを当該交換データと対応づけて記憶手段に格納し、第2のモジュールでは、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを記憶手段から取り出し、取り出した第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証することとしたので、交換データの改ざんを防止することができる。

【0017】また、請求項3に記載の発明にかかるセキュア情報交換システムは、請求項2に記載の発明において、前記第1のモジュールが、複数の交換データを含むリストについての第2の改ざん検知コードを算定する第2の算定手段と、前記第2の算定手段により算定された第2の改ざん検知コードを前記リストとともに前記記憶手段に格納する第2の格納手段と、を備え、前記第2のモジュールが、前記第2の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第2の検証手段をさらに備えたことを特徴とする。

【0018】この請求項3に記載の発明によれば、第1のモジュールでは、複数の交換データを含むリストについての第2の改ざん検知コードを算定し、算定した第2

の改ざん検知コードをリストとともに記憶手段に格納し、第2のモジュールでは、第2の改ざん検知コードに基づいてリストの改ざんの有無を検証することとしたので、交換データをリスト構造で格納する場合にも、このリストの改ざんを効率よく防止することができる。

【0019】また、請求項4に記載の発明にかかるセキュア情報交換システムは、請求項1～3に記載の発明において、前記第1のモジュールおよび第2のモジュールが、前記記憶手段に記憶した交換データの編集要求並びに削除要求を拒否する拒否手段をさらに備えたことを特徴とする。

【0020】この請求項4に記載の発明によれば、第1のモジュールおよび第2のモジュールが、記憶手段に記憶した交換データの編集要求並びに削除要求を拒否することとしたので、交換データが編集や削除される被害を防止することができる。

【0021】また、請求項5に記載の発明にかかるセキュア情報交換システムは、請求項1～4に記載の発明において、前記第1のモジュールが、前記第1の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成する作成手段と、前記受取証作成手段により作成された受取証データを前記第1の端末装置に返送する返送手段と、をさらに備えたことを特徴とする。

【0022】この請求項5に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第1の端末装置に返送することとしたので、交換データの受付を効率よく証明することができるとともに、該交換データの授受にかかる責任の所在を明らかにすることができる。

【0023】また、請求項6に記載の発明にかかるセキュア情報交換システムは、請求項5に記載の発明において、前記作成手段が、前記交換データの特徴量を含む受取証データを作成することを特徴とする。

【0024】この請求項6に記載の発明によれば、交換データの特徴量を含む受取証データを作成することとしたので、交換データと受取証の不整合を効率よく防止することができる。

【0025】また、請求項7に記載の発明にかかるセキュア情報交換システムは、請求項5～6に記載の発明において、前記作成手段が、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする。

【0026】この請求項7に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成することとしたので、該当する交換データを効率よく記憶手段から検索することができる。

【0027】また、請求項8に記載の発明にかかるセキュア情報交換システムは、請求項5～7に記載の発明に

において、前記作成手段が、前記受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成することを特徴とする。

【0028】この請求項8に記載の発明によれば、受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成することとしたので、この受取証データ自体の改ざんについても防止することができる。

【0029】また、請求項9に記載の発明にかかるセキュア情報交換システムは、請求項5～8に記載の発明において、前記第1のモジュールが、前記第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第2の端末装置に送出済みであるか否かを確認する送出確認手段と、前記送出確認手段による確認結果を前記第1の端末装置に通知する送出確認通知手段と、をさらに備えたことを特徴とする。

【0030】この請求項9に記載の発明によれば、第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第2の端末装置に送出済みであるか否かを確認し、この確認結果を第1の端末装置に通知することとしたので、送信確認を効率よくおこなうことができる。

【0031】また、請求項10に記載の発明にかかるセキュア情報交換システムは、請求項5～9に記載の発明において、前記第1のモジュールが、前記第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶手段に記憶されているか否かを確認する記憶確認手段と、前記記憶確認手段により前記記憶手段に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶手段から削除する削除手段と、前記交換データの削除の有無を前記第1の端末装置に通知する削除通知手段と、をさらに備えたことを特徴とする。

【0032】この請求項10に記載の発明によれば、第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶手段に記憶されているか否かを確認し、記憶手段に当該交換データが記憶されていることが確認された際に、当該交換データを記憶手段から削除し、交換データの削除の有無を第1の端末装置に通知することとしたので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことができる。

【0033】また、請求項11に記載の発明にかかるセキュア情報交換システムは、請求項1～10に記載の発明において、前記第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードが、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする。

【0034】この請求項11に記載の発明によれば、第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードを、装置内部に保持した秘密鍵を用いて算定した電子署名とすることとしたので、迅速かつ効率よく改ざんを防止することができる。

【0035】また、請求項12に記載の発明にかかるセキュア情報交換システムは、請求項1～11に記載の発明において、前記第1のモジュールおよび第2のモジュールが、耐タンパー性を有する筐体に格納されたことを特徴とする。

【0036】この請求項12に記載の発明によれば、第1のモジュールおよび第2のモジュールを耐タンパー性を有する筐体に格納することとしたので、該第1のモジュールおよび第2のモジュール自体に対する不正な行為を防止することができる。

【0037】また、請求項13に記載の発明にかかるセキュア情報交換方法は、第1のネットワーク上に位置する第1の端末装置と第2のネットワーク上に位置する第2の端末装置との間で情報交換をおこなうセキュア情報交換方法において、前記第1の端末装置から交換データを受け付けた際に、該交換データを所定の記憶部に格納する格納工程と、前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶部から取り出して当該第2の端末装置に出力する出力工程と、を含んだことを特徴とする。

【0038】この請求項13に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データを記憶部に格納し、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶部から取り出して当該第2の端末装置に出力することとしたので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができる。

【0039】また、請求項14に記載の発明にかかるセキュア情報交換方法は、請求項13に記載の発明において、前記格納工程が、前記第1の端末装置から交換データを受け付ける受付工程と、前記受付工程により受け付けられた交換データについての第1の改ざん検知コードを算定する第1の算定工程と、前記第1の算定工程により算定された第1の改ざん検知コードを当該交換データと対応づけて前記記憶部に格納する第1の格納工程と、を含み、前記出力工程が、前記第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを前記記憶部から取り出す取出工程と、前記取出工程により取り出された第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第1の検証工程と、を含んだことを特徴とする。

【0040】この請求項14に記載の発明によれば、第

1の端末装置から交換データを受け付け、受け付けた交換データについての第1の改ざん検知コードを算定し、算定した第1の改ざん検知コードを当該交換データと対応づけて記憶部に格納し、一方、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを記憶部から取り出し、取り出した第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証することとしたので、交換データの改ざんを防止することができる。

【0041】また、請求項15に記載の発明にかかるセキュリティ情報交換方法は、請求項14に記載の発明において、前記格納工程が、複数の交換データを含むリストについての第2の改ざん検知コードを算定する第2の算定工程と、前記第2の算定工程により算定された第2の改ざん検知コードを前記リストとともに前記記憶部に格納する第2の格納工程と、を含み、前記出力工程が、前記第2の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第2の検証工程をさらに含んだことを特徴とする。

【0042】この請求項15に記載の発明によれば、複数の交換データを含むリストについての第2の改ざん検知コードを算定し、算定した第2の改ざん検知コードをリストとともに記憶部に格納し、第2のモジュールが、第2の改ざん検知コードに基づいてリストの改ざんの有無を検証することとしたので、交換データをリスト構造で格納する場合であっても、このリストの改ざんを効率よく防止することができる。

【0043】また、請求項16に記載の発明にかかるセキュリティ情報交換方法は、請求項13～15に記載の発明において、前記記憶部に記憶した交換データの編集要求並びに削除要求を拒否する拒否工程をさらに含んだことを特徴とする。

【0044】この請求項16に記載の発明によれば、記憶部に記憶した交換データの編集要求並びに削除要求を拒否できるとしたので、交換データが編集や削除される被害を防止することができる。

【0045】また、請求項17に記載の発明にかかるセキュリティ情報交換方法は、請求項13～16に記載の発明において、前記格納工程が、前記第1の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成する作成工程と、前記受取証作成工程により作成された受取証データを前記第1の端末装置に返送する返送工程と、をさらに含んだことを特徴とする。

【0046】この請求項17に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第1の端末装置に返送することとしたので、交換データの受付を効率よく証明することが

できるとともに、該交換データの授受にかかる責任の所在を明らかにすることができる。

【0047】また、請求項18に記載の発明にかかるセキュリティ情報交換方法は、請求項17に記載の発明において、前記作成工程が、前記交換データの特徴量を含む受取証データを作成することを特徴とする。

【0048】この請求項18に記載の発明によれば、交換データの特徴量を含む受取証データを作成することとしたので、交換データと受取証の不整合を効率よく防止することができる。

【0049】また、請求項19に記載の発明にかかるセキュリティ情報交換方法は、請求項17～18に記載の発明において、前記作成工程が、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする。

【0050】この請求項19に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成することとしたので、該当する交換データを効率よく記憶手段から検索することができる。

【0051】また、請求項20に記載の発明にかかるセキュリティ情報交換方法は、請求項17～19に記載の発明において、前記作成工程が、前記受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成することを特徴とする。

【0052】この請求項20に記載の発明によれば、受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成することとしたので、この受取証データ自体の改ざんについても防止することができる。

【0053】また、請求項21に記載の発明にかかるセキュリティ情報交換方法は、請求項17～20に記載の発明において、前記格納工程が、前記第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第2の端末装置に送出済みであるか否かを確認する送出確認工程と、前記送出確認工程による確認結果を前記第1の端末装置に通知する送出確認通知工程と、をさらに含んだことを特徴とする。

【0054】この請求項21に記載の発明によれば、第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第2の端末装置に送出済みであるか否かを確認し、この確認結果を第1の端末装置に通知することとしたので、送信確認を効率よくおこなうことができる。

【0055】また、請求項22に記載の発明にかかるセキュリティ情報交換方法は、請求項17～21に記載の発明において、前記格納工程が、前記第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶部に記憶さ

れているか否かを確認する記憶確認工程と、前記記憶確認工程により前記記憶部に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶部から削除する削除工程と、前記交換データの削除の有無を前記第1の端末装置に通知する削除通知工程と、をさらに含んだことを特徴とする。

【0056】この請求項22に記載の発明によれば、第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶部に記憶されているか否かを確認し、記憶部に当該交換データが記憶されていることが確認された際に、当該交換データを記憶部から削除し、交換データの削除の有無を第1の端末装置に通知することとしたので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことができる。

【0057】また、請求項23に記載の発明にかかるセキュア情報交換方法は、請求項13～22に記載の発明において、前記第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードが、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする。

【0058】この請求項23に記載の発明によれば、第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードを、装置内部に保持した秘密鍵を用いて算定した電子署名とすることとしたので、迅速かつ効率よく改ざんを防止することができる。

【0059】また、請求項24に記載の発明にかかる記録媒体は、請求項13～23のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項13～23のいずれか一つの動作をコンピュータによって実現することができる。

【0060】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるセキュア情報交換システム、セキュア情報交換方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0061】（セキュア情報交換システムの概念）まず最初に、本実施の形態で用いるセキュア情報交換システムの概念について説明する。図1は、本実施の形態で用いるセキュア情報交換システムの概念を説明するための説明図である。

【0062】図1示すように、このセキュア情報交換システムは、インターネットなどの外部ネットワーク1と内部ネットワーク2の間にセキュア情報交換装置10を配設したシステム構成となり、このセキュア情報交換装置10内部には、外部用モジュール10a、内部用モジュール10bおよび大容量記憶装置13を有している。

【0063】このセキュア情報交換装置10は、外部ネ

ットワーク1または内部ネットワーク2の一方から外部用モジュール10aまたは内部用モジュール10bが交換データを受け取り、これを一時的に大容量記憶装置13に保存する。そして、他方のネットワークから交換データの取り出しを要求されると、外部用モジュール10aまたは内部用モジュール10bが保存した交換データを他方のネットワークに渡す。

【0064】このように、かかるセキュア情報交換装置10では、ストア・リトリブ（Store and Retrieve）方式を採用している。ここで、この大容量記憶装置13は、論理窓口の役割を果たすことになる。なお、セキュア情報交換装置10内部の大容量記憶装置13に保存された交換データに不正なアクセスがおこなわれないように、このセキュア情報交換装置10は交換データを保護する機能も有する。

【0065】したがって、かかるセキュア交換システムを用いれば、異なるセキュリティポリシーを持つ2つのネットワークシステムの独立性を完全に保ったまま、双方のネットワークシステム間でオフラインメディアと人手を介さない情報交換が可能となる。

【0066】また、このセキュア情報交換システムでは、セキュア情報交換装置10に交換データを送り届けるまでが送信者側の責任であり、このセキュア情報交換装置10から交換データを取り出した後は受信者側の責任とすることができるので、責任範囲が明確となる。

【0067】図2は、図1に示したセキュア情報交換装置10の配置位置の一例を示す図である。同図に示すように、住民基本台帳ネットワーク20と、基幹LAN21と、情報系LAN22と、インターネット23とをそれぞれ接続する場合には、住民基本台帳ネットワーク20～基幹LAN21の間と、基幹LAN21～情報系LAN22の間と、情報系LAN22～インターネット23の間とにそれぞれセキュア情報交換装置10を配設することにより、各ネットワークの独立性を保持することになる。

【0068】（セキュア情報交換装置の装置構成）つぎに、図1に示したセキュア情報交換装置10の装置構成について具体的に説明する。図3は、図1に示したセキュア情報交換装置10の装置構成を示すブロック図である。

【0069】同図に示すように、外部モジュール10aが、外部ネットワーク1を介して該外部ネットワーク1上の端末装置11によりアクセスされ、内部モジュール10bが内部ネットワーク2を介して該内部ネットワーク2上の端末装置12によりアクセスされる。そして、この外部モジュール10aおよび内部モジュール10bは、物理的な耐タンパー性を有する筐体100に格納され、それぞれ大容量記憶装置13にデータを記憶することができる。

【0070】外部モジュール10aは、通信ポート11

0、一時記憶部111、内部記憶媒体112、プロセッサ113、内部タイマ114およびプログラム格納媒体115からなり、内部モジュール10bは、通信ポート120、一時記憶部121、内部記憶媒体122、プロセッサ123、内部タイマ124およびプログラム格納媒体125からなる。

【0071】通信ポート110または120は、外部システムまたは内部システムとの通信をするためのインターフェース部であり、たとえばイーサネット（登録商標）カードなどが該当する。ただし、外部ネットワーク1と内部ネットワーク2とで通信プロトコルが異なる場合もある。特に、基幹系のネットワークはイーサネットであるとは限らない。

【0072】一時記憶部111または121は、プロセッサ113または123が処理するデータを一時記憶するメモリであり、読み書き可能なRAMが該当する。この一時記憶部111には、電源が断にされた際に消去されても良いデータが記憶される。

【0073】内部記憶媒体112または122は、外部モジュール10aまたは内部モジュール10bの内部管理データなどを記憶する二次記憶媒体であり、ハードディスク装置などが該当する。

【0074】プロセッサ113または123は、プログラム格納媒体115または125からプログラムをロードして実行するCPUであり、内部タイマ114または124は、現在時刻を計時してプロセッサ113または123に供給するタイマである。

【0075】プログラム格納媒体115または125は、セキュア情報交換装置10が提供する情報交換サービスのプログラムが格納された媒体であり、ROMやハードディスク装置が該当する。

【0076】耐タンパー筐体100は、セキュア情報交換装置10のプログラムや内部管理データ、タイマなどを不正に改ざん、消去されないよう、これらを外部からの物理的な攻撃から保護するための物理的な筐体である。なお、この耐タンパー筐体100を無理に開けられた際には、内部管理データを消去したり、システム管理者に通報するよう構成することができる。また、システム管理者には開けることができないが、保守要員であれば開けられる鍵をかけることもできる。

【0077】大容量記憶装置13は、このセキュア情報交換装置10が接続する双方のネットワーク（外部ネットワーク1および内部ネットワーク2）から渡される交換データを格納する二次記憶装置であり、ハードディスク装置などが該当する。交換データ保護の観点からRAIDとすることもできる。

【0078】なお、この大容量記憶装置13は、大容量のデータ交換がおこなわれるような場合には耐タンパー筐体100内に収まらない可能性が高いので、ここでは耐タンパー筐体100の外部に配設することとしたが、

耐タンパー筐体100の内部に配設しても良い。

【0079】（セキュア情報交換装置の機能および処理内容）つぎに、図1に示したセキュア情報交換装置10の機能および処理内容について説明する。このセキュア情報交換装置10は、（a）データ交換機能、（b）交換データ保護機能を有する。

【0080】ここで、（a）データ交換機能とは、一方のネットワークから交換データを受け取り、他方のネットワークからのデータ取り出し要求に対してその交換データを渡す機能である。なお、一方のネットワークから受け取った交換データを他方のネットワークに自動的に転送することはない。他方のネットワークからデータが取り出されるまで交換データを大容量記憶装置13に保持する。

【0081】（b）交換データ保護機能とは、内部に保持されている交換データが不正に改ざんされないよう該交換データを安全に保護する機能であり、一方のネットワークから受け取った交換データは、他方のネットワークから取り出されるまで内部に保持される。

【0082】また、このセキュア情報交換装置10は、図1に示したセキュア情報交換装置10の機能および処理内容に示すように（1）サービス受付処理、（2）ストア処理、（3）交換データ一覧処理、（4）リトリブ処理および（5）送出確認処理をおこなう。このサービス受付処理とは、セキュア情報交換装置10にアクセスするユーザから様々なサービス処理要求を受け付け、その要求内容に応じて処理を割り振るものである。

【0083】ストア処理とは、セキュア情報交換装置10に対して送信された交換データを受け取ってシステム内部にストアする処理であり、交換データ一覧処理とは、セキュア情報交換装置10内部で保持している交換データの識別番号の一覧を取得する処理である。

【0084】リトリブ処理とは、セキュア情報交換装置10に対して送られた取り出し要求に対して、システム内部に保持されている交換データを送出する処理であり、送出確認処理とは、セキュア情報交換装置10に対して送信された交換データが、すでに他方のネットワークで取り出されたか否かを確認する処理である。

【0085】このように、かかるセキュア情報交換装置10は、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうための機能を有している。以下、これらの処理の処理手順について順次説明する。

【0086】（1）サービス受付処理

つぎに、図1に示したセキュア情報交換装置10がおこなうサービス受け付け処理手順について具体的に説明する。図5は、図1に示したセキュア情報交換装置10がおこなうサービス受け付け処理手順を示すフローチャートである。

【0087】同図に示すように、このセキュア情報交換

装置10は、まず最初にユーザが認証されているか否かを確認し(ステップS501)、ユーザが認証されていない場合には(ステップS501否定)、サービス処理要求がユーザ認証処理要求であるか否かを調べる(ステップS502)。

【0088】その結果、ユーザ認証処理要求である場合には(ステップS502肯定)、ユーザ認証処理をおこなった後に(ステップS503)処理を終了し、ユーザ認証処理要求でない場合には(ステップS502否定)、エラー処理をおこなった後に(ステップS512)処理を終了する。

【0089】これに対して、ユーザが認証されている場合には(ステップS501肯定)、サービス処理要求がストア処理要求であるか否かを調べ(ステップS504)、ストア処理要求である場合には(ステップS504肯定)、ストア処理をおこなって(ステップS505)処理を終了する。

【0090】また、サービス処理要求がストア処理要求ではない場合には(ステップS504否定)、該サービス処理要求が交換データ一覧処理要求であるか否かを調べ(ステップS506)、交換データ一覧処理要求である場合には(ステップS506肯定)、交換データ一覧処理をおこなった後に(ステップS507)処理を終了する。

【0091】また、サービス処理要求が交換データ一覧処理要求ではない場合には(ステップS506否定)、このサービス処理要求がリトリート処理要求であるか否かを調べ(ステップS508)、リトリート処理要求である場合には(ステップS508肯定)、リトリート処理をおこなった後に(ステップS509)処理を終了する。

【0092】また、サービス処理要求がリトリート処理要求ではない場合には(ステップS508否定)、このサービス処理要求が送出確認処理要求であるか否かを調べ(ステップS510)、送出確認処理要求である場合には(ステップS510肯定)、送出確認処理要求をおこなった後に(ステップS511)処理を終了する。なお、サービス処理要求が送出確認処理要求ではない場合には(ステップS510否定)、エラー処理をおこなった後に(ステップS512)、処理を終了する。

【0093】つぎに、図5のステップS503に示したユーザ認証処理手順についてさらに詳細に説明する。図6は、図5のステップS503に示したユーザ認証処理手順を示すフローチャートである。なおここでは、簡単なパスワード認証をおこなう場合を示すこととし、アカウント管理データは図7に示すように外部ネットワーク1用、内部ネットワーク2用に別々に内部記憶媒体112および122に記憶されるものとする。

【0094】図6に示すように、まず最初に、内部記憶媒体112または122に記憶されたアカウント管理デ

ータを参照し(ステップS601)、このアカウント管理データの中で受け取ったアカウント名に対応するアカウントエントリを検索する(ステップS602)。

【0095】そして、アカウントエントリが存在しない場合には(ステップS603否定)、エラー処理をおこなった(ステップS607)後に、処理を終了する。一方、アカウントエントリが存在する場合には(ステップS603肯定)、受け取ったパスワードとアカウントエントリにあるパスワードを照合する(ステップS604)。

【0096】その結果、パスワードが一致した場合には(ステップS605肯定)、ユーザ認証済みであることを一時記憶部111または121で記憶する(ステップS606)。一方、ステップS605において、パスワードが一致しない場合には(ステップS605否定)、エラー処理をおこなった(ステップS607)のちに、処理を終了する。

【0097】(2) ストア処理

つぎに、図1に示したセキュア情報交換装置10がおこなうストア処理手順について具体的に説明する。図8は、図1に示したセキュア情報交換装置10がおこなうストア処理手順を示すフローチャートであり、図9は、かかるストア処理の概念を説明するための説明図である。

【0098】図8に示すように、このセキュア情報交換装置10は、まず最初にユーザのアカウント名、受け取った論理窓口番号、アクセス種別(ストア)を元に後述する窓口アクセス権検査処理をおこない(ステップS801)、アクセス権があるか否かを確認する(ステップS802)。

【0099】その結果、アクセス権がない場合には(ステップS802否定)、エラー処理をおこなった後に(ステップS810)処理を終了する。一方、ステップS802において、アクセス権がある場合には(ステップS802肯定)、受け取った交換データに交換データ識別番号を割り当て(ステップS803)、受け取った交換データに対して電子署名を計算し(ステップS804)、論理窓口番号、交換データ識別番号、電子署名を元に交換データリスト追加処理をおこなう(ステップS805)。

【0100】そして、交換データ更新処理が成功したか否かを確認し(ステップS806)、失敗に終わった場合には(ステップS806否定)、エラー処理をおこなった(ステップS810)後に、すべての処理を終了する。

【0101】これに対して、交換データ更新処理が成功した場合(ステップS806肯定)には、交換データを大容量記憶装置13の論理窓口番号に対応するディレクトリに交換データ識別番号をファイル名として格納し(ステップS807)、交換データ識別番号と格納した

論理窓口番号、電子署名を元に受取証作成処理をおこなう(ステップS808)、作成された受取証データを交換データ送信元のユーザに送る(ステップS809)。

【0102】たとえば、図9に示す外部用モジュール10aが、コンピュータ11からストア要求、論理窓口番号および交換データを受け取ると、「20000328-00000327」という交換データ識別番号を付与するとともに、その電子署名を計算して、大容量記憶装置13の該当する論理窓口に交換データリストファイルを格納して、受取証データをコンピュータ11を使用する交換データ送信元のユーザに送信することになる。

【0103】図10は、かかる交換データリストファイルの構造を示す図であり、同図に示すように、この交換データリストファイルは、交換データ識別番号および交換データ電子署名からなるN個の交換データエントリ#1〜#Nと、交換データリストに対する電子署名とからなる。

【0104】図11は、受取証データの構造を示す図である。この図11からもわかるように、かかる受取証データは、交換データ識別番号、格納した論理窓口番号および交換データ電子署名からなる受取内容と、その受取内容に対する電子署名とからなる。

【0105】なお、ここではコンピュータ11とセキュア情報交換装置10との間でのネットワークセキュリティについての説明を省略したが、SSL(Secure Sockets Layer)などの既存の安全な通信プロトコルを使用することもできる。

【0106】また、ここでは受け取った交換データの内容についての説明を省略したが、交換データの内容についてコンテンツフィルタリングを実行することもできる。これにより、たとえば基幹系ネットワークから情報漏洩などが起こらないようにすることができる。

【0107】つぎに、図8のステップS801に示した窓口アクセス権検査処理手順について説明する。図12は、図8のステップS801に示した窓口アクセス権検査処理手順を示すフローチャートであり、図13は、論理窓口管理データの構造を示す図である。

【0108】図12に示すように、この窓口アクセス権検査処理では、論理窓口データを内部記憶媒体から読み出し(ステップS1201)、受け取った論理窓口番号に対応する論理窓口管理データの管理エントリを参照して(ステップS1202)、管理エントリの内容がアカウント名、アクセス種別に適合しているか否かを調べる(ステップS1203)。

【0109】そして、管理エントリの内容がアカウント名、アクセス種別に適合していない場合には(ステップS1203否定)、エラー処理をおこなった後に(ステップS1204)処理を終了する。

【0110】この処理は、ユーザのアカウント名と論理窓口番号、アクセス種別(ストア、リトリブ、一覧)

を受け取って処理する。論理窓口ごとに設定されているデータ交換方向とアクセス種別がマッチしなければアクセスを拒否することになる。なお、データ交換方向とは、一方のネットワークから他方のネットワークヘデータを交換する方向のことを意味し、どちらの方向にデータ交換をおこなえるかが論理窓口ごとにあらかじめ設定されている。

【0111】かかる論理窓口管理データは、図13に示すようにN個のアクセス許可エントリ#1〜#Nからなるアクセス許可リスト、論理窓口番号、データ交換方向からなる複数の管理エントリを有する。

【0112】つぎに、図8のステップS805に示した交換データリスト追加処理手順について説明する。図14は、図8のステップS805に示した交換データリスト追加処理手順を示すフローチャートである。

【0113】同図に示すように、この交換データリスト追加処理では、大容量記憶装置13から論理窓口番号に対応する交換データリストファイルを読み出し(ステップS1401)、その後、交換データリスト検証処理をおこなう(ステップS1402)。

【0114】そして、検証に失敗した場合(ステップS1403否定)には、エラー処理をおこなった(ステップS1408)後に、処理を終了する。これに対して、検証に成功した場合には(ステップS1403肯定)、受け取った交換データ識別番号と電子署名で新しい交換データエントリを作成し(ステップS1404)する。

【0115】その後、作成した交換データエントリを交換データリストに追加し(ステップS1405)、交換データリスト署名処理をおこなった後に(ステップS1406)、大容量記憶装置13に交換データリストファイルを格納する(ステップS1407)。

【0116】つぎに、図14のステップS1402に示した交換データリスト検証処理手順について説明する。図15は、図14のステップS1402に示した交換データリスト検証処理手順を示すフローチャートである。

【0117】同図に示すように、この交換データリスト検証処理は、交換データリストファイルの正当性を検証するものであり、具体的には、交換データリストファイルに格納されている電子署名を参照し(ステップS1501)、交換データリストファイルに格納されている交換データリストに対してハッシュ値を計算し(ステップS1502)、内部記憶媒体に格納されている公開鍵で電子署名を復号して検証用ハッシュ値を得る(ステップS1503)。

【0118】その後、ハッシュ値と検証用ハッシュ値が一致するか否かを確認し(ステップS1504)、一致しない場合には(ステップS1504否定)、エラー処理をおこなった後に(ステップS1505)処理を終了する。

【0119】つぎに、図14のステップS1406に示

した交換データリスト署名処理手順について説明する。図 16 は、図 14 のステップ S1406 に示した交換データリスト署名処理手順を示すフローチャートである。

【0120】同図に示すように、この交換データリスト署名処理では、交換データリストに対してハッシュ値を計算し（ステップ S1601）、内部記憶媒体に格納されている秘密鍵でハッシュ値を暗号化して電子署名を得た後（ステップ S1602）、交換データリストに電子署名を付与して交換データリストファイルとする（ステップ S1603）。

【0121】つぎに、図 8 のステップ S808 に示した受取証の作成処理手順について説明する。図 17 は、図 8 のステップ S808 に示した受取証の作成処理手順を示すフローチャートである。

【0122】同図に示すように、この受取証の作成処理では、受け取った交換データ識別番号と論理窓口番号、交換データ電子署名をあわせて受取内容を作成し（ステップ S1701）、この受取内容に対してはハッシュ値を計算する（ステップ S1702）。

【0123】その後、内部記憶媒体に格納されている秘密鍵でハッシュ値を暗号化して電子署名を取得し（ステップ S1703）、受取内容に電子署名を付与して受取証とする（ステップ S1704）。

【0124】つぎに、受取証の検証処理について説明する。図 18 は受取証の検証処理手順を示すフローチャートである。同図に示すように、まず最初に受け取った受取証から電子署名を取り出すとともに（ステップ S1801）、受け取った受取証から受取内容を取り出し（ステップ S1802）、受取内容に対してハッシュ値を計算する（ステップ S1803）。

【0125】その後、内部記憶媒体に格納されている公開鍵で電子署名を復号して検証用ハッシュ値を取得し（ステップ S1804）、ハッシュ値と検証用ハッシュ値とを比較する（ステップ S1805）。その結果、ハッシュ値と検証用ハッシュ値とが異なる場合には（ステップ S1805 肯定）、エラー処理をおこなって（ステップ S1806）処理を終了し、両者が一致する場合には（ステップ S1805 否定）正常終了する。

【0126】（3）交換データ一覧処理
つぎに、図 1 に示したセキュア情報交換装置 10 がおこなう交換データ一覧処理手順について具体的に説明する。図 19 は、図 1 に示したセキュア情報交換装置 10 がおこなう交換データ一覧処理手順を示すフローチャートである。

【0127】同図に示すように、このセキュア情報交換装置 10 は、ユーザのアカウント名、受け取った論理窓口番号、アクセス種別（一覧）を元に窓口アクセス権検査処理をおこない（ステップ S1901）、アクセス権があるか否かを確認する（ステップ S1902）。

【0128】そして、アクセス権がない場合には（ステ

ップ S1902 否定）、エラー処理をおこなった後に（ステップ S1908）処理を終了し、アクセス権がある場合には（ステップ S1902 肯定）、受け取った論理窓口番号に対応する交換データリストファイルを大容量記憶装置 13 から読み出し（ステップ S1903）、交換データリスト検証処理をおこなう（ステップ S1904）。

【0129】その結果、検証に失敗した場合には（ステップ S1905 否定）、エラー処理をおこなった（ステップ S1908）後に、処理を終了し、検証に成功した場合には（ステップ S1905 肯定）、交換データリストファイルから交換データ識別番号をすべて取り出し、交換データ識別番号リストを作成し（ステップ S1906）、該交換データ識別番号リストをユーザ側に返す（ステップ S1907）。

【0130】（4）リトリート処理

つぎに、図 1 に示したセキュア情報交換装置 10 がおこなうリトリート処理手順について具体的に説明する。図 20 は、図 1 に示したセキュア情報交換装置 10 がおこなうリトリート処理手順を示すフローチャートである。この処理は、ユーザから論理窓口番号と交換データ識別番号を受け取る。

【0131】同図に示すように、セキュア情報交換装置 10 は、ユーザのアカウント名、受け取った論理窓口番号、アクセス種別（リトリート）を元に窓口アクセス権検査処理をおこない（ステップ S2001）、アクセス権があるか否かを確認する（ステップ S2002）。

【0132】その結果、アクセス権がない場合には（ステップ S2002 否定）、エラー処理をおこなった後に（ステップ S2008）処理を終了し、アクセス権がある場合には（ステップ S2002 肯定）、論理窓口番号に対応するディレクトリから交換データ識別番号に対応する交換データを読み出し（ステップ S2003）、交換データ識別番号、交換データを元に交換データリスト削除処理をおこない（ステップ S2004）、処理が成功したか否かを確認する（ステップ S2005）。

【0133】そして、処理が失敗した場合には（ステップ S2005 否定）、エラー処理をおこなった後に（ステップ S2008）処理を終了し、処理が成功した場合には（ステップ S2005 肯定）、交換データファイルを大容量記憶装置 13 の論理窓口番号に対応するディレクトリから削除し（ステップ S2006）、交換データをユーザに送信する（ステップ S2007）。

【0134】つぎに、図 20 のステップ S2004 に示した交換データの削除処理手順について説明する。図 21 は、図 20 のステップ S2004 に示した交換データの削除処理手順を示すフローチャートである。この処理は、論理窓口番号、交換データ識別番号、交換データを受け取り、交換データリストから該当する交換データエントリを削除するものである。

【0135】同図に示すように、この交換データの削除処理では、論理窓口番号に対応する交換データリストファイルを大容量記憶装置13から読み出し（ステップS2101）、交換データリスト検証処理をおこない（ステップS2102）、検証に成功したか否かを確認する（ステップS2103）。

【0136】その結果、検証に失敗した場合には（ステップS2103否定）、エラー処理をおこなった後に（ステップS2112）処理を終了し、検証に成功した場合には（ステップS2103肯定）、受け取った交換データ識別番号に該当する交換データエントリを交換データリストから取得するとともに（ステップS2104）、交換データエントリから交換データ電子署名を取り出す（ステップS2105）。

【0137】その後、内部記憶媒体に格納されている公開鍵で交換データ電子署名を復号して検証用ハッシュ値とするとともに（ステップS2106）、受け取った交換データについてのハッシュ値を計算し（ステップS2107）、ハッシュ値と検証用ハッシュ値が一致するかどうかを確認する（ステップS2108）。

【0138】その結果、両者が一致しない場合には（ステップS2108否定）、エラー処理をおこなった後に（ステップS2112）処理を終了し、両者が一致する場合には（ステップS2108肯定）、交換データリストから先の交換データエントリを削除し（ステップS2109）、交換データリスト署名処理をおこなった後に（ステップS2110）、大容量記憶装置2111に交換データリストファイルを格納する（ステップS2111）。

【0139】（5）送出確認処理

つぎに、図1に示したセキュア情報交換装置10がおこなう送出確認処理手順について具体的に説明する。図22は、図1に示したセキュア情報交換装置10がおこなう送出確認処理手順を示すフローチャートである。この処理は、ユーザから受取証を受け取り、これに対応する交換データが他方のネットワークに送出されたかどうかを確認するものである。

【0140】同図に示すように、このセキュア情報交換装置10では、受け取った受取証を元に受取証検証処理をおこない（ステップS2201）、検証に成功したか否かを確認する（ステップS2202）。

【0141】その結果、検証に失敗した場合（ステップS2202否定）には、エラー処理をおこなった後に（ステップS2212）処理を終了し、検証に成功した場合には（ステップS2202肯定）、受取証から受取内容を取り出し（ステップS2203）、この受取内容から論理窓口番号と交換データ識別番号を取り出す（ステップS2204）。

【0142】その後、大容量記憶装置13から論理窓口番号に対応する交換データリストファイルを読み出し

（ステップS2205）、交換データリスト検証処理をおこなった後に（ステップS2206）、検証に成功したか否かを確認する（ステップS2207）。

【0143】その結果、検証に失敗した場合（ステップS2207否定）には、エラー処理をおこなった（ステップS2212）後に、処理を終了する。一方、検証に成功した場合には（ステップS2207肯定）、交換データリストファイルから交換データ識別番号に対応する交換データエントリを取り出し（ステップS2208）、対応する交換データエントリが存在するか否かを確認する（ステップS2209）。

【0144】そして、対応する交換データエントリが存在する場合（ステップS2209肯定）には、交換データは他方のネットワークに送出されていないことをユーザに通知し（ステップS2210）、対応する交換データエントリが存在しない場合には（ステップS2209否定）、交換データが他方のネットワークに送出されたことをユーザに通知する（ステップS2211）。

【0145】上述してきたように、本実施の形態では、外部用モジュール10aが外部ネットワーク1から交換データを受け付けた際に、該交換データを大容量記憶装置13に格納し、内部用モジュール10bが内部ネットワーク2から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを大容量記憶装置13から取り出して出力するセキュア情報交換装置10を設けるよう構成したので人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができる。

【0146】なお、一般的な情報システムがおこなうように、処理した内容をログとして記録することもできる。この場合には、記録したログをデータ交換をおこなった証拠とできるよう、交換データと同様にログにも電子署名を施すことが望ましい。

【0147】また、場合によっては、送出確認だけでなく、送信取消の処理をおこなうよう構成することもできる。また、交換データが大容量記憶装置10に格納されている間に、交換データを送り込んだユーザが受取証を提示して送信取消を要求した場合には、装置内部に保持した交換データを取り消すように構成することになる。

【0148】なお、取り消されたのか、他方のネットワークに送出したのかを明確にするために、取り消した交換データについては別途取消リストのようなもので管理する必要がある。

【0149】また、交換データをストアする際に、その交換データに対して保持期限を設定できるようにすることもできる。その保持期限を過ぎてもリトリブされない場合には、保持期限が過ぎたことをストアしたユーザに通知したうえでその交換データを削除することになる。

【0150】また、一方のネットワークにある原本性保

証電子保存システムから電子原本を受け取り、他方のネットワークからその電子原本の受取要求があれば、その電子原本をその他方のネットワークにある原本性保証電子保存システムに送出するよう構成することもできる。

【0151】なお、本実施の形態で説明したセキュア情報交換方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータで実行することによって実現される。このプログラムは、HD（ハードディスク）、FD（フロッピーディスク）、CD-ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって、実行される。また、このプログラムは、インターネットなどのネットワークを介して配布することが可能な伝送媒体であってもよい。

【0152】

【発明の効果】以上説明したように、請求項1に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データを記憶手段に格納し、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶手段から取り出して当該第2の端末装置に出力するセキュア情報交換装置を第1のネットワークおよび第2のネットワークの間に配設するよう構成したので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことが可能なセキュア情報交換システムが得られるという効果を奏する。

【0153】また、請求項2に記載の発明によれば、第1のモジュールでは、第1の端末装置から交換データを受け付け、受け付けた交換データについての第1の改ざん検知コードを算定し、算定した第1の改ざん検知コードを当該交換データと対応づけて記憶手段に格納し、第2のモジュールでは、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを記憶手段から取り出し、取り出した第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証するよう構成したので、交換データの改ざんを防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0154】また、請求項3に記載の発明によれば、第1のモジュールでは、複数の交換データを含むリストについての第2の改ざん検知コードを算定し、算定した第2の改ざん検知コードをリストとともに記憶手段に格納し、第2のモジュールでは、第2の改ざん検知コードに基づいてリストの改ざんの有無を検証するよう構成したので、交換データをリスト構造で格納する場合にも、このリストの改ざんを効率よく防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0155】また、請求項4に記載の発明によれば、第

1のモジュールおよび第2のモジュールが、記憶手段に記憶した交換データの編集要求並びに削除要求を拒否するよう構成したので、交換データが編集や削除される被害を防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0156】また、請求項5に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第1の端末装置に返送するよう構成したので、交換データの受付を効率よく証明することができるとともに、該交換データの授受にかかる責任の所在を明らかにすることが可能なセキュア情報交換システムが得られるという効果を奏する。

【0157】また、請求項6に記載の発明によれば、交換データの特徴量を含む受取証データを作成するよう構成したので、交換データと受取証の不整合を効率よく防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0158】また、請求項7に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成するよう構成したので、該当する交換データを効率よく記憶手段から検索することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0159】また、請求項8に記載の発明によれば、受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成するよう構成したので、この受取証データ自体の改ざんについても防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0160】また、請求項9に記載の発明によれば、第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第2の端末装置に送出済みであるか否かを確認し、この確認結果を第1の端末装置に通知するよう構成したので、送信確認を効率よくおこなうことが可能なセキュア情報交換システムが得られるという効果を奏する。

【0161】また、請求項10に記載の発明によれば、第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶手段に記憶されているか否かを確認し、記憶手段に当該交換データが記憶されていることが確認された際に、当該交換データを記憶手段から削除し、交換データの削除の有無を第1の端末装置に通知するよう構成したので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことが可能なセキュア情報交換システムが得られるという効果を奏する。

【0162】また、請求項11に記載の発明によれば、第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードを、装置内部に保持した秘密鍵を用

いて算定した電子署名とするよう構成したので、迅速かつ効率よく改ざんを防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0163】また、請求項12に記載の発明によれば、第1のモジュールおよび第2のモジュールを耐タンパー性を有する筐体に格納するよう構成したので、該第1のモジュールおよび第2のモジュール自体に対する不正な行為を防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【0164】また、請求項13に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データを記憶部に格納し、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶部から取り出して当該第2の端末装置に出力するよう構成したので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことが可能なセキュア情報交換方法が得られるという効果を奏する。

【0165】また、請求項14に記載の発明によれば、第1の端末装置から交換データを受け付け、受け付けた交換データについての第1の改ざん検知コードを算定し、算定した第1の改ざん検知コードを当該交換データと対応づけて記憶部に格納し、一方、第2の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第1の改ざん検知コードを記憶部から取り出し、取り出した第1の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証するよう構成したので、交換データの改ざんを防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【0166】また、請求項15に記載の発明によれば、複数の交換データを含むリストについての第2の改ざん検知コードを算定し、算定した第2の改ざん検知コードをリストとともに記憶部に格納し、第2のモジュールでは、第2の改ざん検知コードに基づいてリストの改ざんの有無を検証するよう構成したので、交換データをリスト構造で格納する場合にも、このリストの改ざんを効率よく防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【0167】また、請求項16に記載の発明によれば、記憶部に記憶した交換データの編集要求並びに削除要求を拒否できるとしたので、交換データが編集や削除される被害を防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【0168】また、請求項17に記載の発明によれば、第1の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第1の端末装置に返送するよう構成したので、交換データの受付を効率よく証明することができるとともに、該交換データの授受にかかる責任

の所在を明らかにすることが可能なセキュア情報交換方法が得られるという効果を奏する。

【0169】また、請求項18に記載の発明によれば、交換データの特徴量を含む受取証データを作成するよう構成したので、交換データと受取証の不整合を効率よく防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【0170】また、請求項19に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成するよう構成したので、該当する交換データを効率よく記憶手段から検索することが可能なセキュア情報交換方法が得られるという効果を奏する。

【0171】また、請求項20に記載の発明によれば、受取証データの受取内容についての第3の改ざん検知コードを生成し、該生成した第3の改ざん検知コードを含む受取証データを作成するよう構成したので、この受取証データ自体の改ざんについても防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【0172】また、請求項21に記載の発明によれば、第1の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第2の端末装置に送出済みであるか否かを確認し、この確認結果を第1の端末装置に通知するよう構成したので、送信確認を効率よくおこなうことが可能なセキュア情報交換方法が得られるという効果を奏する。

【0173】また、請求項22に記載の発明によれば、第1の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶部に記憶されているか否かを確認し、記憶部に当該交換データが記憶されていることが確認された際に、当該交換データを記憶部から削除し、交換データの削除の有無を第1の端末装置に通知するよう構成したので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことが可能なセキュア情報交換方法が得られるという効果を奏する。

【0174】また、請求項23に記載の発明によれば、第1の改ざん検知コード、第2の改ざん検知コードまたは第3の検知コードを、装置内部に保持した秘密鍵を用いて算定した電子署名とするよう構成したので、迅速かつ効率よく改ざんを防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【0175】また、請求項24に記載の発明によれば、請求項13～23のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項13～23のいずれか一つの動作をコンピュータによって実現することが可能な記録媒体が得られるという効果を奏する。

【図面の簡単な説明】

【図1】この発明の本実施の形態で用いるセキュア情報

交換システムの概念を説明するための説明図である。

【図 2】この発明の本実施の形態の図 1 に示したセキュア情報交換装置の配置位置の一例を示す説明図である。

【図 3】この発明の本実施の形態の図 1 に示したセキュア情報交換装置の装置構成を示すブロック図である。

【図 4】この発明の本実施の形態の図 1 に示したセキュア情報交換装置の処理内容の一覧を示す説明図である。

【図 5】この発明の本実施の形態の図 1 に示したセキュア情報交換装置がおこなうサービス受け付け処理手順を示すフローチャートである。

【図 6】この発明の本実施の形態の図 5 のステップ S 503 に示したユーザ認証処理手順を示すフローチャートである。

【図 7】この発明の本実施の形態のセキュア情報交換装置のアカウント管理データの構成を示す説明図である。

【図 8】この発明の本実施の形態の図 1 に示したセキュア情報交換装置がおこなうストア処理手順を示すフローチャートである。

【図 9】この発明の本実施の形態のセキュア情報交換装置のストア処理の概念を説明するための説明図である。

【図 10】この発明の本実施の形態の交換データリストファイルの構造を示す説明図である。

【図 11】この発明の本実施の形態のセキュア情報交換装置の受取証データの構造を示す説明図である。

【図 12】この発明の本実施の形態の図 8 のステップ S 801 に示した窓口アクセス権検査処理手順を示すフローチャートである。

【図 13】この発明の本実施の形態のセキュア情報交換装置の論理窓口管理データの構造を示す説明図である。

【図 14】この発明の本実施の形態の図 8 のステップ S 805 に示した交換データリスト追加処理手順を示すフローチャートである。

【図 15】この発明の本実施の形態の図 14 のステップ S 1402 に示した交換データリスト検証処理手順を示すフローチャートである。

【図 16】この発明の本実施の形態の図 14 のステップ S 1406 に示した交換データリスト署名処理手順を示すフローチャートである。

【図 7】

アカウントインリ #1	アカウント名
	パスワード
アカウントインリ #2	
...	
アカウントインリ #N	

【図 17】この発明の本実施の形態の図 8 のステップ S 808 に示した受取証の作成処理手順を示すフローチャートである。

【図 18】この発明の本実施の形態の受取証の検証処理手順を示すフローチャートである。

【図 19】この発明の本実施の形態の図 1 に示したセキュア情報交換装置がおこなう交換データ一覧処理手順を示すフローチャートである。

10 【図 20】この発明の本実施の形態の図 1 に示したセキュア情報交換装置がおこなうリトリブ処理手順を示すフローチャートである。

【図 21】この発明の本実施の形態の図 20 のステップ S 2004 に示した交換データの削除処理手順を示すフローチャートである。

【図 22】この発明の本実施の形態の図 1 に示したセキュア情報交換装置がおこなう送出確認処理手順を示すフローチャートである。

【図 23】従来の典型的なファイアウォールの概念を説明するための説明図である。

20 【符号の説明】

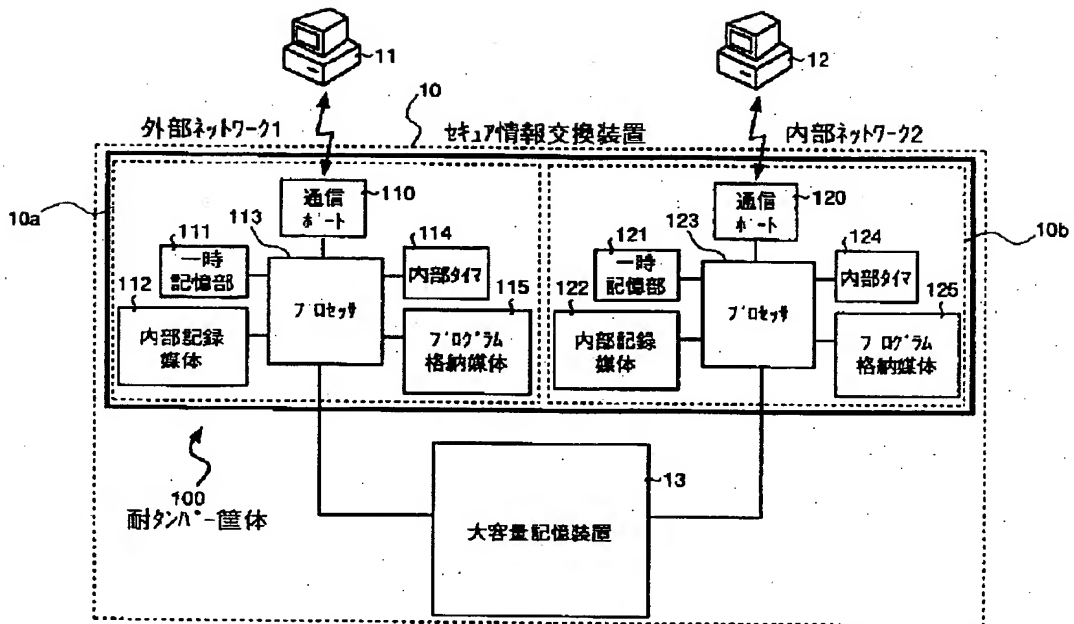
- 1 外部ネットワーク
- 2 内部ネットワーク
- 10 セキュア情報交換装置
- 10a 外部モジュール
- 10b 内部モジュール
- 11 コンピュータ
- 11, 12 端末装置
- 13 大容量記憶装置
- 20 住民基本台帳ネットワーク
- 30 100 耐タンパー筐体
- 100 筐体
- 110, 120 通信ポート
- 111, 121 一時記憶部
- 112, 122 内部記憶媒体
- 113, 123 プロセッサ
- 114, 124 内部タイマ
- 115, 125 プログラム格納媒体

【図 11】

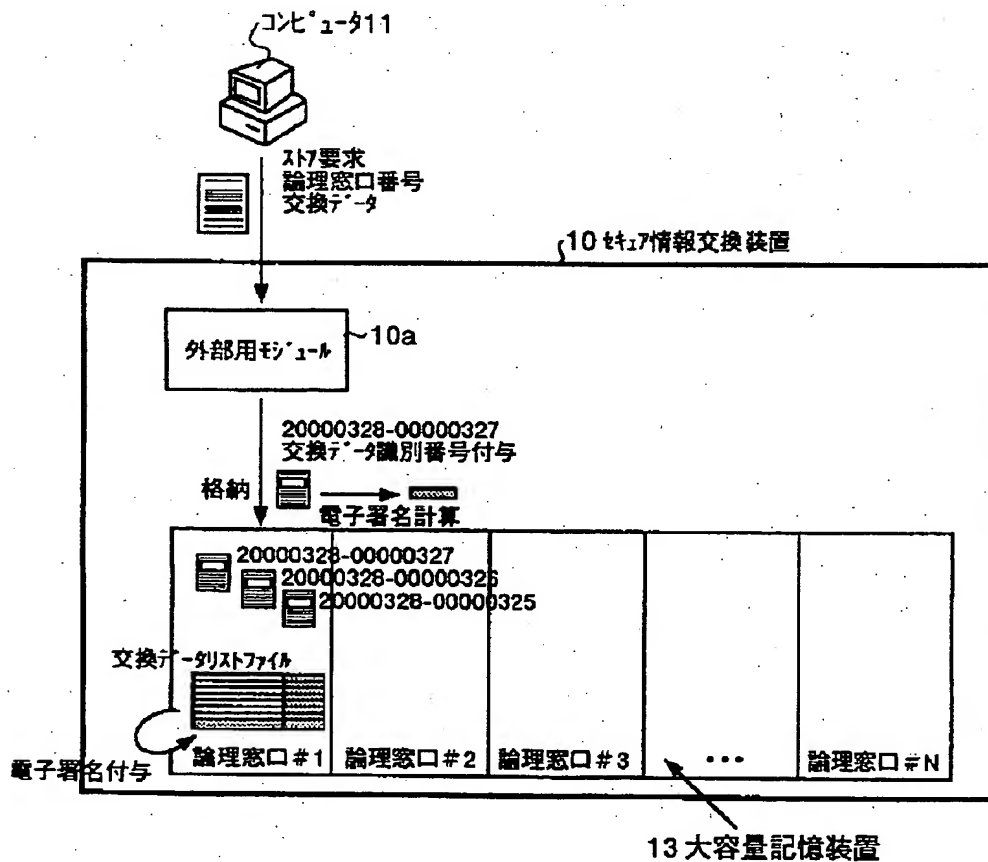
受取内容	交換データ識別番号
	格納した論理窓口番号
	交換データ電子署名
受取内容に対する電子署名	

処理名	処理内容
サービス受付処理	セキュリティ情報交換装置にアクセスするユーザから様々なサービス処理要求を受け付け、その要求内容に応じて処理を割り振るものである。
ストア処理	セキュリティ情報交換装置に対して送信された交換データを受け取ってシステム内部にストアする処理である。
交換データ一覧処理	セキュリティ情報交換装置内部で保持している交換データの識別番号の一覧を取得する処理である。
リトリフ処理	セキュリティ情報交換装置に対して送られた取り出し要求に対して、システム内部に保持されている交換データを送出する処理である。
送出確認処理	セキュリティ情報交換装置に対して送信された交換データが、すでに他方のネットワークで取り出されたかどうかを確認する処理である。

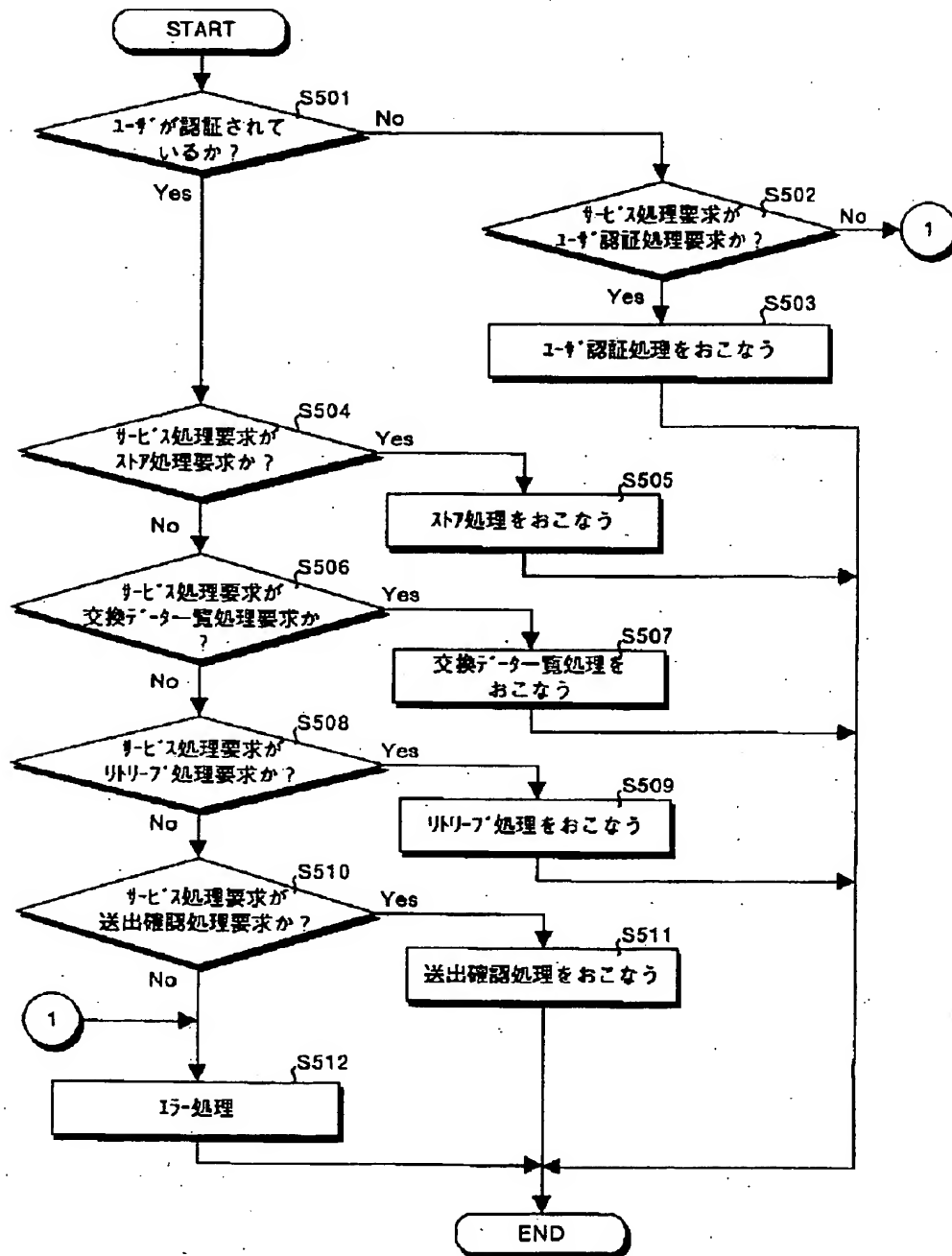
【図3】



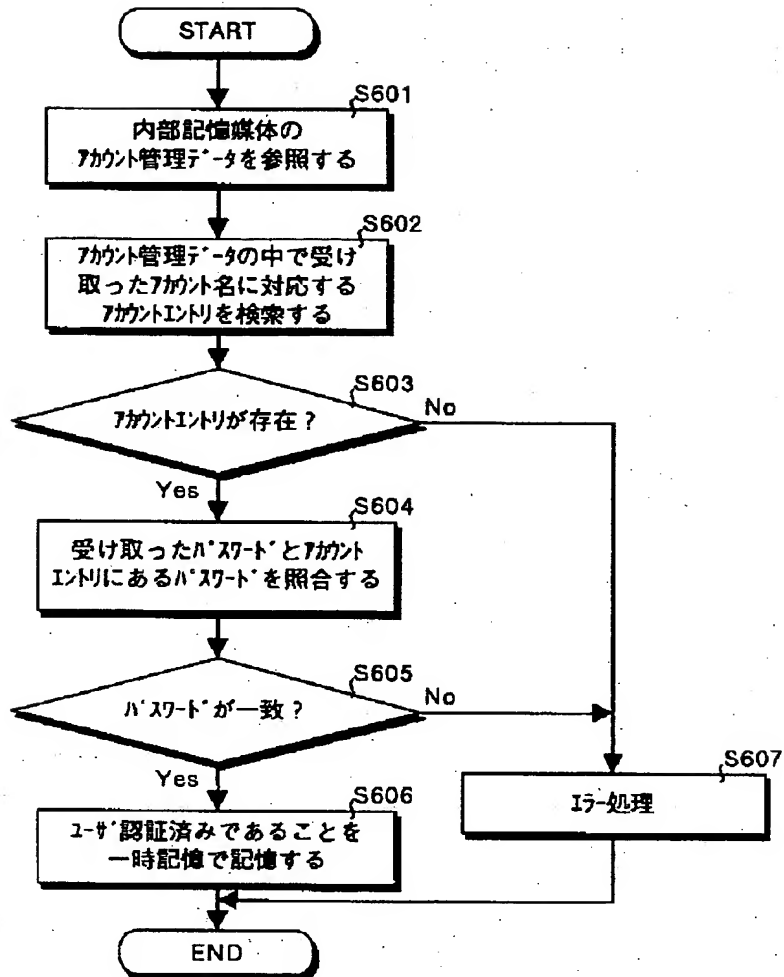
【図9】



【図5】



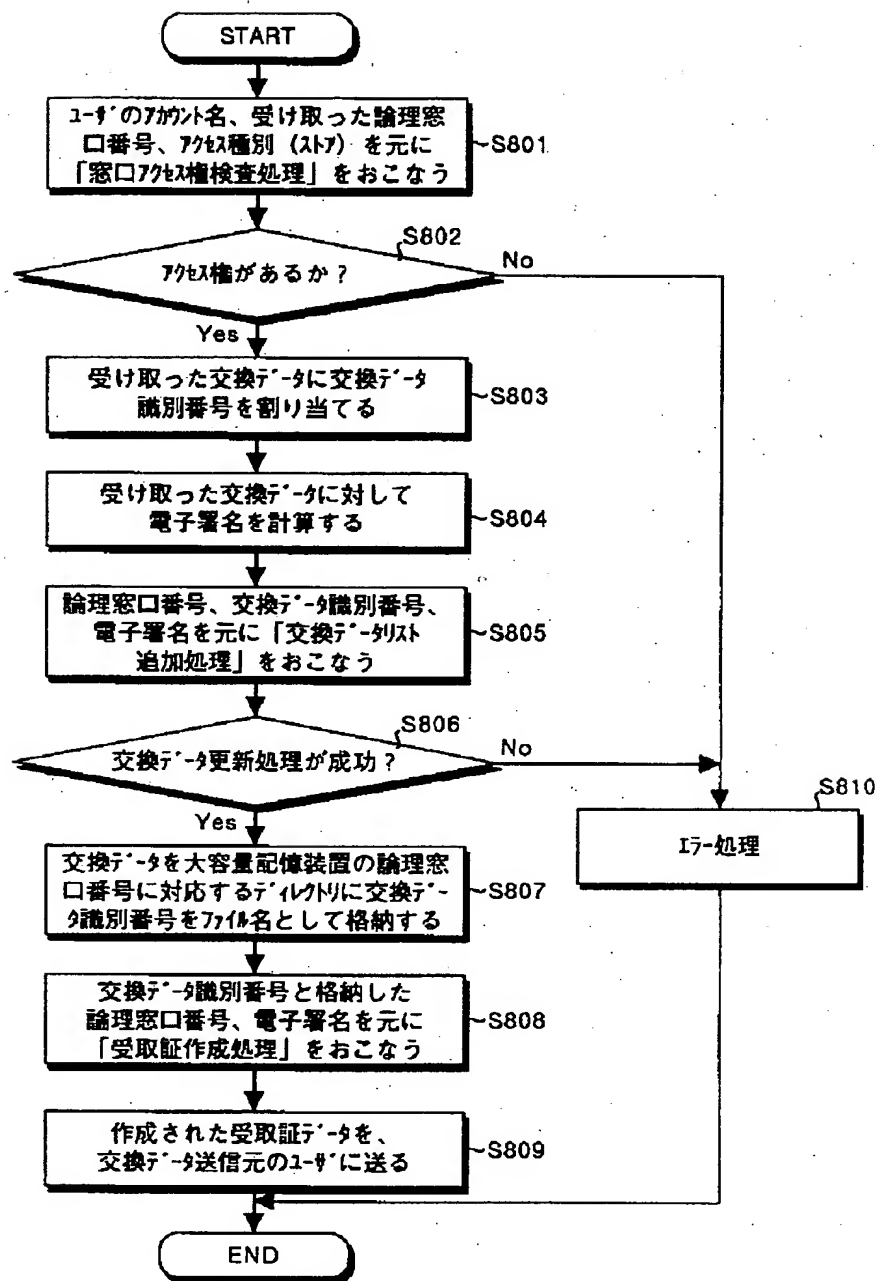
【図6】



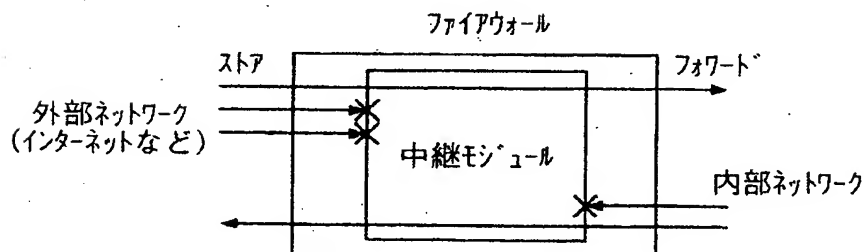
【図10】

交換データリスト	交換データID # 1	交換データ識別番号
		交換データ電子署名
	交換データID # 2	
	...	
	交換データID # N	
交換データリストに対する電子署名		

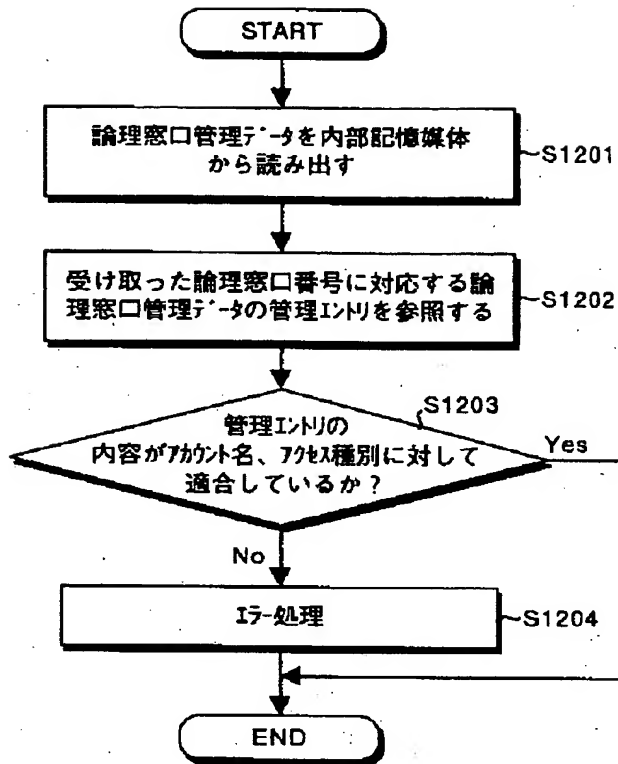
【図8】



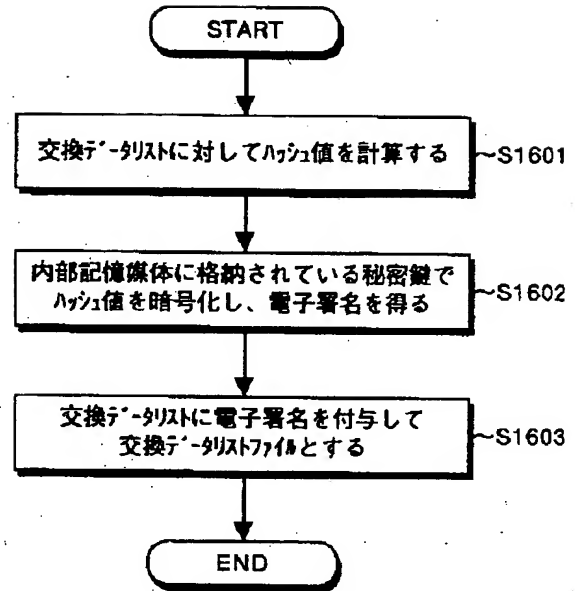
【図23】



【図12】



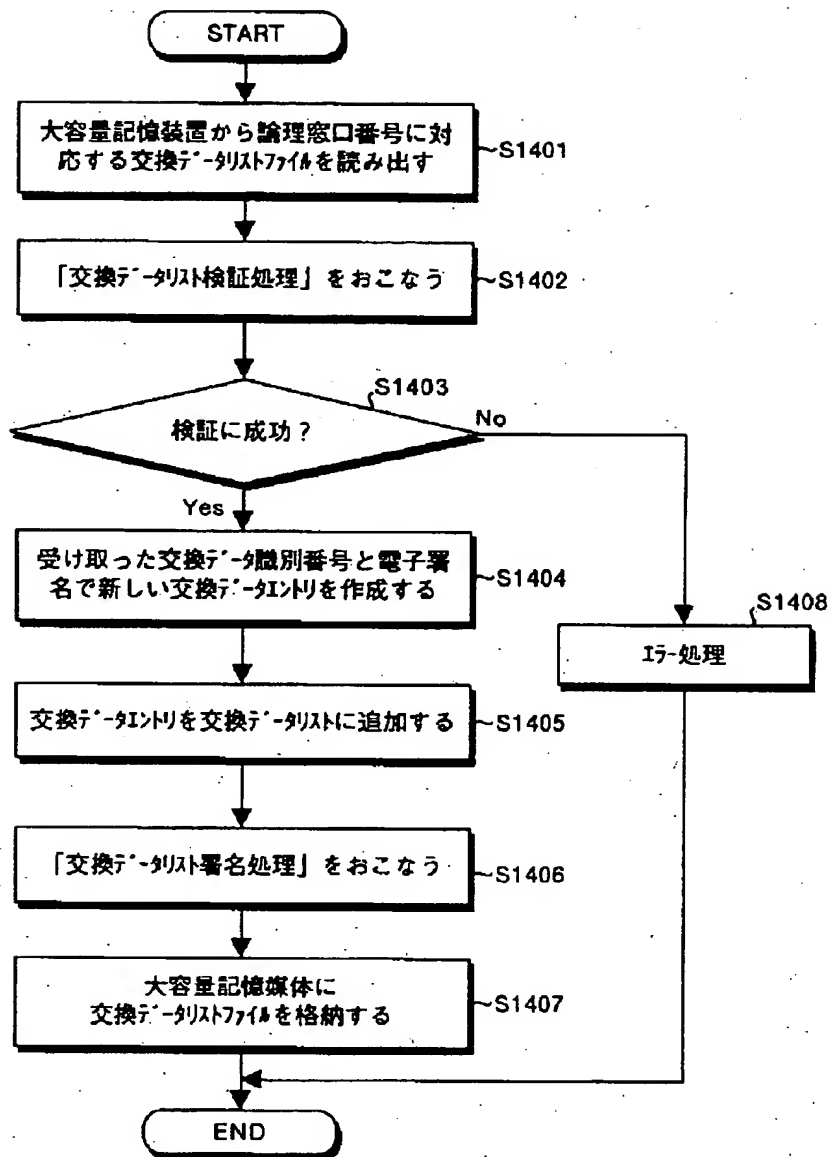
【図16】



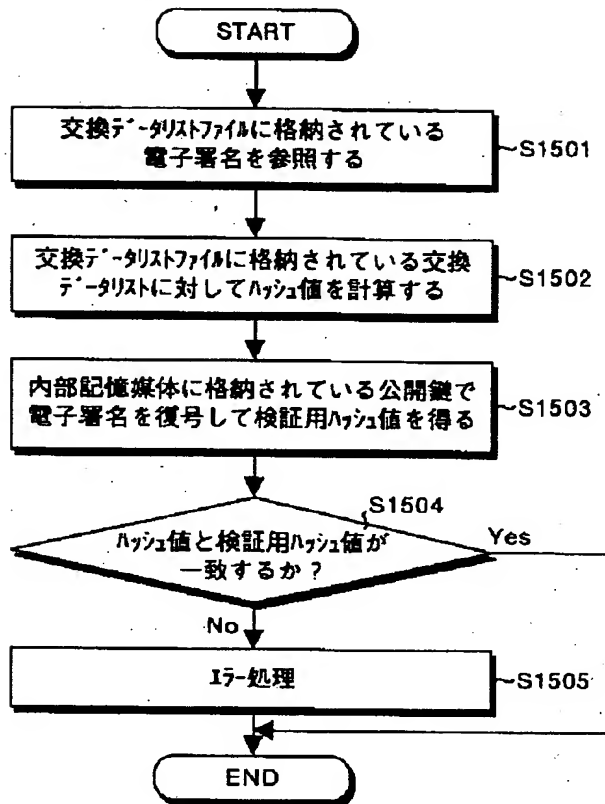
【図13】

管理エントリ # 1	論理窓口番号		
	データ交換方向		
	アクセス許可リスト	アクセス許可エントリ # 1	アカウント名
		アクセス許可エントリ # 2	
		...	
アクセス許可エントリ # N			
管理エントリ # 2			
...			
管理エントリ # N			

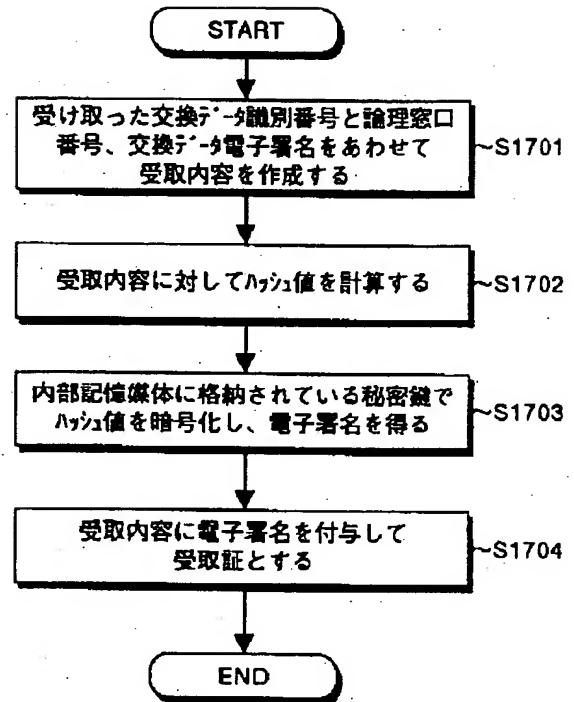
【図 14】



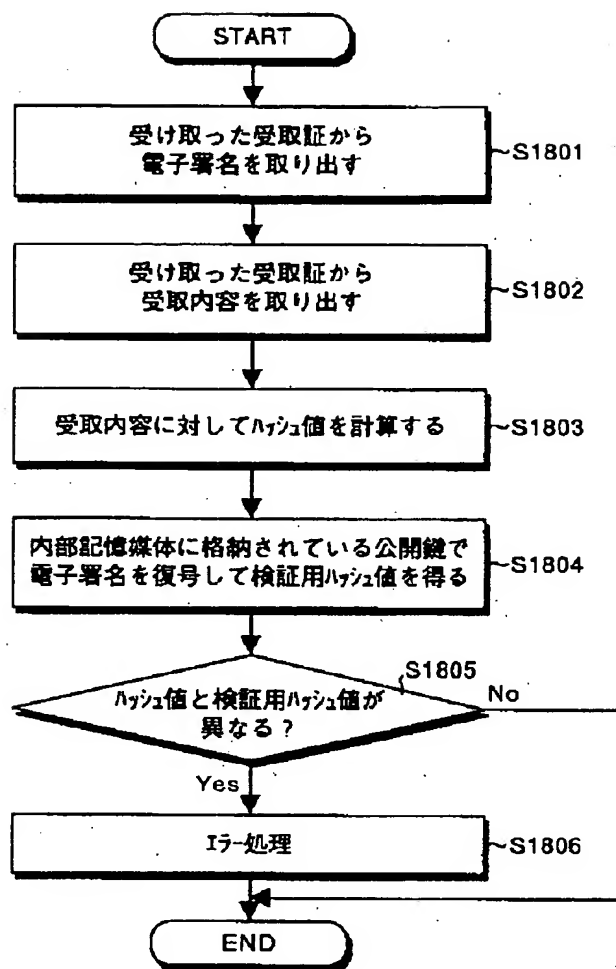
【図15】



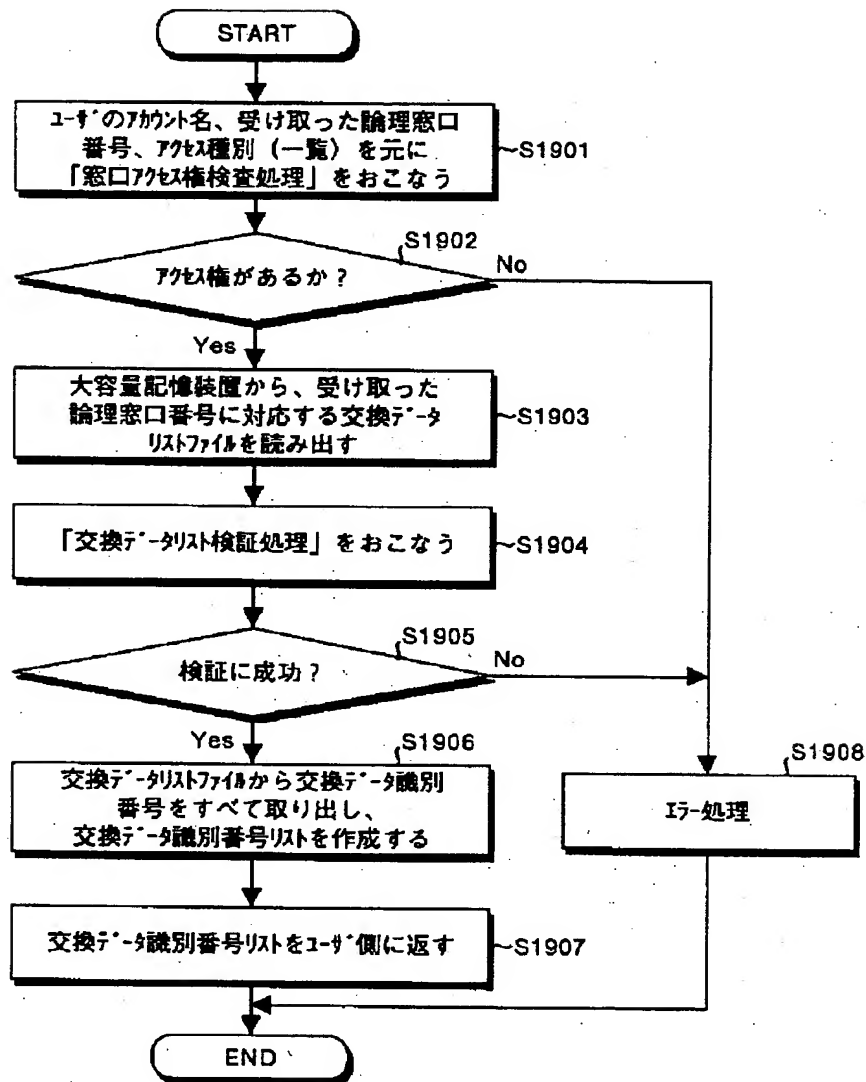
【図17】



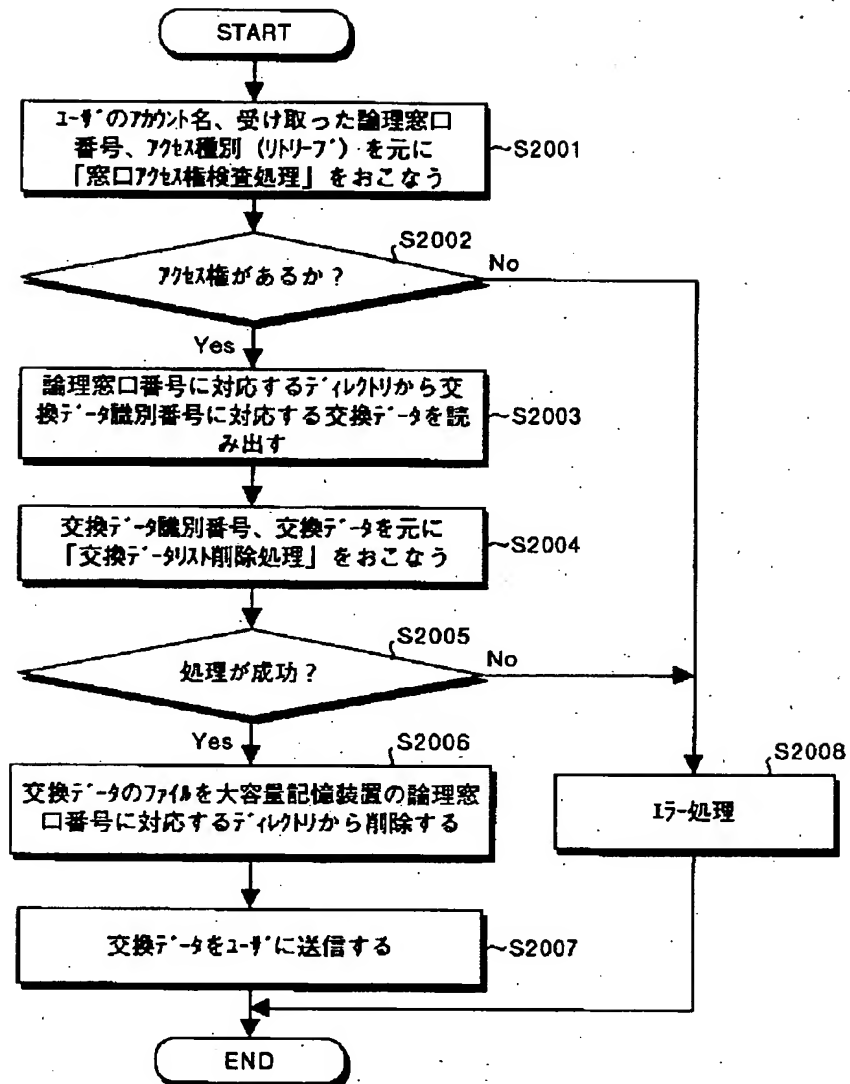
【図18】



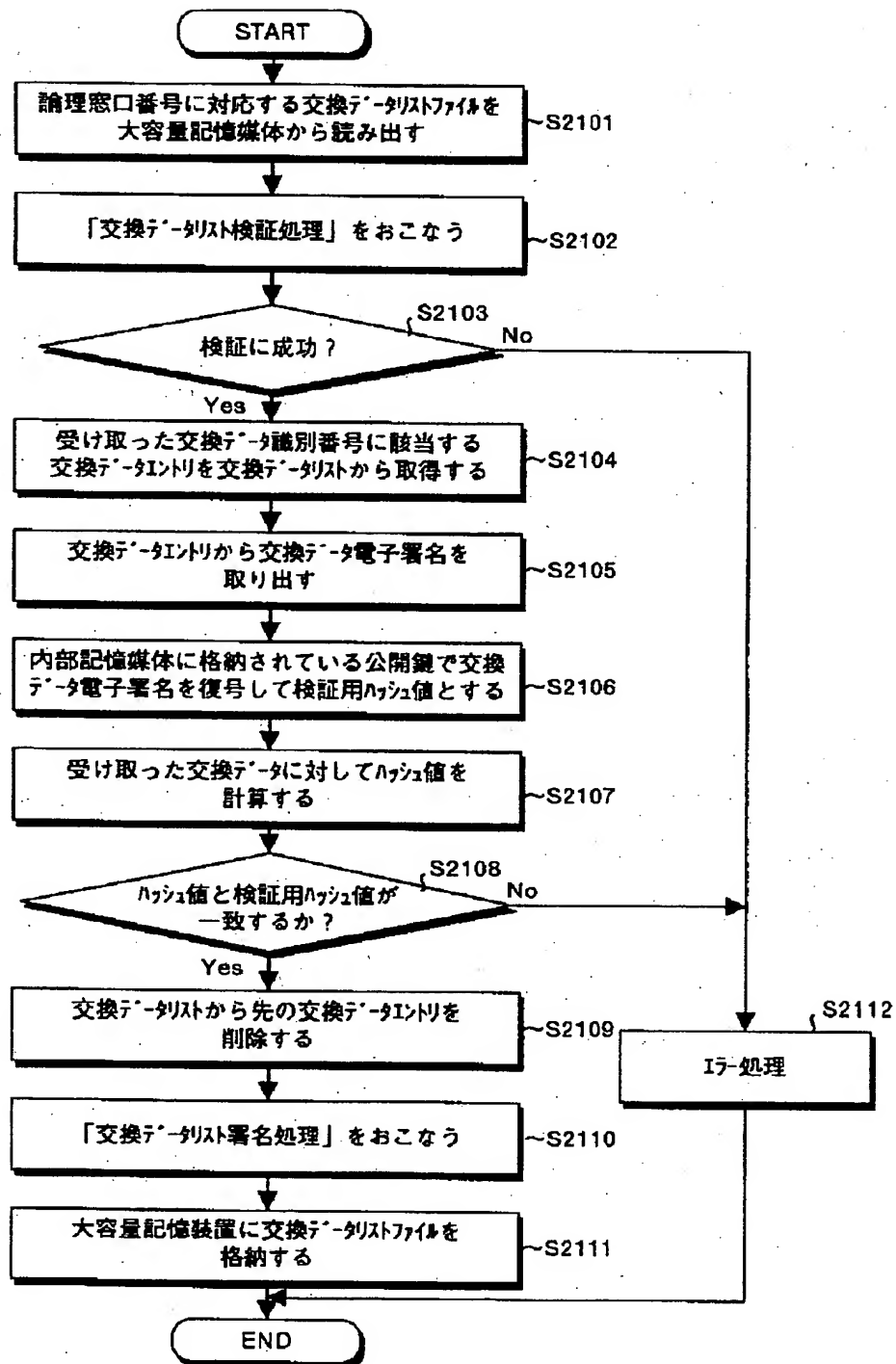
【図19】



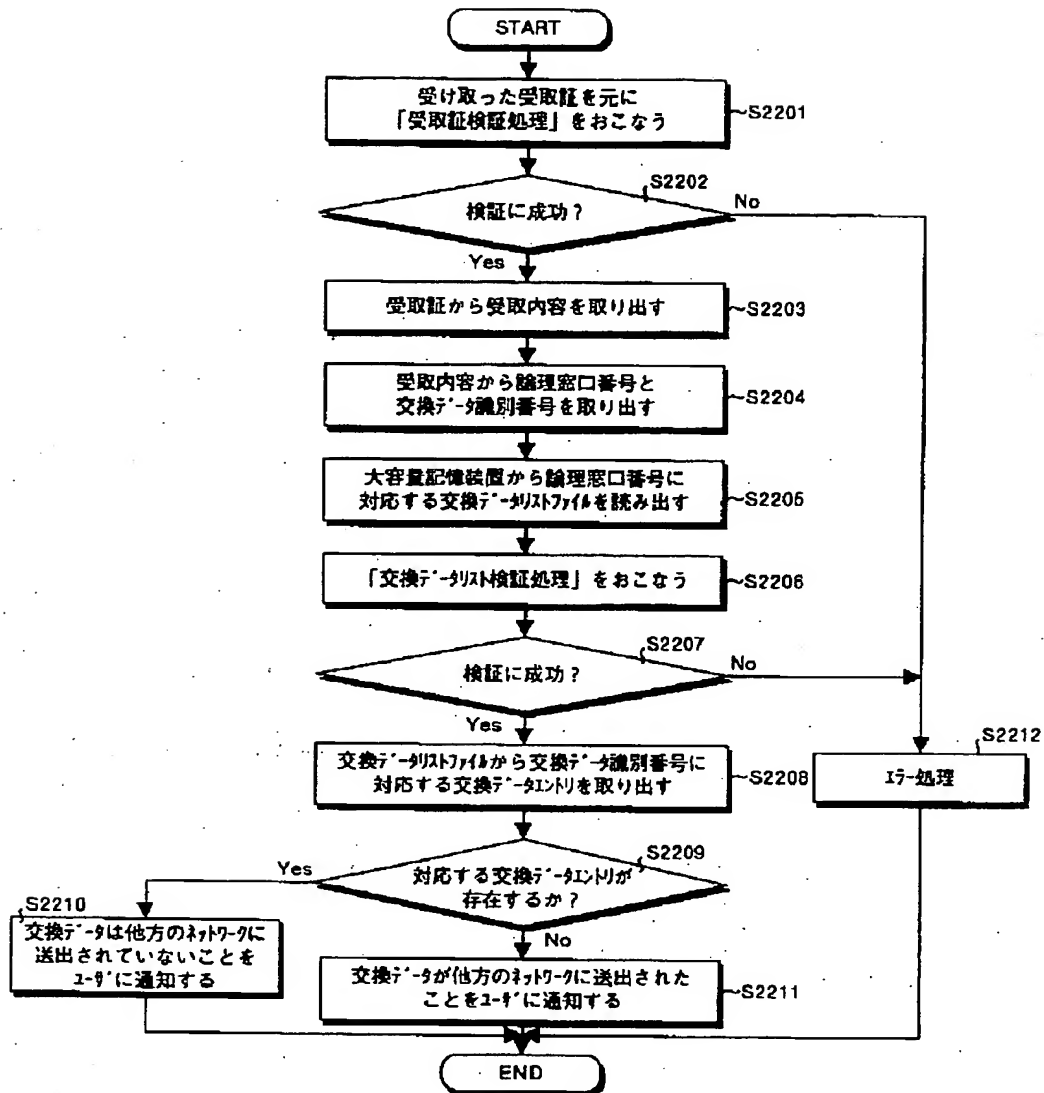
【図20】



【図21】



【図 22】



フロントページの続き

(72)発明者 谷内田 益義
 東京都大田区中馬込1丁目3番6号 株式
 会社リコー内

Fターム(参考) 5J104 AA09 AA16 AA44 EA17 LA03
 LA06 NA02 NA12 NA27 NA42
 PA07
 5K030 GA15 HA06 HB00 LA00 LD19
 9A001 CC03 CC07 CC08 JJ13 JJ25
 LL03

